SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES AND ACCESS TO JPL'S CONTROLLED FACILITIES

[CT, FP-NR&D, FP-R&D, CIS, LH-T&M, T&MC, FPC, CREI, A-E – 10/05] [NFS 1852.204-76-07/02]

(a) The Subcontractor shall be responsible for Information Technology security for all systems connected to a NASA network or operated by the Subcontractor for NASA, regardless of location. This clause is applicable to all or any part of the Subcontract that includes information technology resources or services in which the Subcontractor must have physical or electronic access to NASA's sensitive information contained in unclassified systems that directly support the mission of the Agency. This includes information technology, hardware, software, and the management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. Examples of tasks that require security provisions include:

(1) Computer control of spacecraft, satellites, or aircraft or their payloads;

(2) Acquisition, transmission or analysis of data owned by NASA with significant replacement cost should the Subcontractor's copy be corrupted; and

(3) Access to NASA networks or computers at a level beyond that granted the general public, e.g. bypassing a firewall.

(b) The Subcontractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this Subcontract. The plan shall describe those parts of the Subcontract to which this clause applies. The Subcontractor's IT Security Plan shall be compliant with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.) and the Government Information Security Reform Act of 2000. The plan shall meet IT security requirements in accordance with Federal and NASA policies and procedures that include, but are not limited to:

(1) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources;

(2) NASA Procedural Guidelines (NPG) 2810.1, Security of Information Technology; and

(3) Chapter 4 of NPG 1620.1B, NASA Security Procedures and Guidelines.

(c) Within 45 days after Subcontract award, the Subcontractor shall submit for approval an IT Security Plan. This plan must be consistent with and further detail the approach contained in the offeror's proposal or sealed bid that resulted in the award of this Subcontract and in compliance with the requirements stated in this Article. The plan, as approved by JPL, shall be incorporated into the Subcontract as a compliance document.

(d) In addition to complying with any functional and technical security requirements set forth in the schedule and the provisions of this Subcontract, the Subcontractor shall request JPL badges for its personnel who require regular, unescorted, or unsupervised physical access to JPL and who need physical access to limited or controlled areas within the facility. In addition, the Subcontractor shall obtain unique electronic identifications (from the JPL Enterprise Information System) for its personnel that need electronic access to JPL systems, programs, and data.

(e) The Subcontractor's personnel, including grantees, research associates, co-op students, and all foreign nationals (including permanent resident aliens), requiring continuing and official unescorted access to NASA facilities, buildings, information, and/or privileged access or limited privileged access to IT systems operated by the Subcontractor for NASA or interconnected to a NASA network shall be screened (security reliability investigation and access determination) at an appropriate level (low risk, moderate risk, or high risk) in accordance with NPG 2810.1, Section 4.5, NPG 1620.1B, Chapter 4, and this Article. Subcontractor personnel WILL NOT be authorized access to NASA facilities, buildings, sensitive information, or IT systems without submission of the following required investigative paperwork to the Subcontractor's Security Office AND "interim" favorable access determination by NASA Security Officials based upon their review of the following investigative paperwork:

(1) NASA National Agency Check (NAC) Form 531 and Form FD-258, fingerprint Card (for low risk positions)

Or

(2) Standard Form 85P (SF – 85P), Questionnaire for Public Trust Positions/BI, and form FD – 258 (for US citizens only and permanent resident aliens in moderate and high risk positions)

(f) Computer Security Requirements. The requirements stated in JPL D-7155, titled, “JPL Information Technology Security Requirements for Computer Systems” (incorporated by reference) apply to all IT assets having an IP address belonging to the “jpl.nasa.gov” domain and to all JPL IT assets operated by the Subcontractor, regardless of theasset’s location or network connectivity. Compliance with these requirements will be monitored by network vulnerability scans and physical audits as required by the JPL IT Security Officer.

(g) Controlled Facilities. JPL facilities, as defined by the NASA Mission Essential Infrastructure Protection Program (MEIPP) (incorporated by reference), are designated as NASA controlled facilities.

(h) Personnel Investigations.

(1) National Investigations/(NAC) Requirements.

(A) All Subcontractor personnel assigned to JPL for computer system administration, computer system maintenance (hardware and/or software), network operation, computer operation, or have access to sensitive information as defined in Appendix A to JPL D-7155, must deliver completed NAC paperwork to the JPL Security Office prior to reporting for work at JPL.

(B) All Subcontractor personnel requiring access to controlled facilities must deliver completed personnel investigation or NAC paperwork to the JPL Security Office prior to reporting for work at JPL.

(C) Personnel investigations and NAC/s require original proof of United States citizenship or eligibility for employment. Subcontractor personnel with existing security clearance based on an investigation current within the last five years are not required to submit personnel investigation NAC forms, if their clearance is under five years old, but the Subcontractor must submit a Classified Visit Request for each individual.

(D) Pre-personnel investigatory NAC Access Requirements. In the absence of information suggesting that pre-investigatory NAC access is not advised, Subcontractor personnel will have access on an interim basis once the completed NAC request forms and all required documents are delivered to the JPL Security Office, Building 310, Room 129.

(i) Security Incident Reporting. The Subcontractor shall promptly report to the JPL Help Desk, (818) 354-4357, any suspected or detected IT security incidents as defined in NPG 2810.1, occurring on any IT Assets, that are required to meet the JPL Computer Security Requirements paragraph.

(j) Laboratory Access.

(1) As a NASA restricted facility, JPL requires that all personnel possess valid identification for unescorted access. Individuals who access the Laboratory on a one-time or infrequent basis are processed as visitors. All visitors are processed through the Visitor Control Center and must possess a valid picture ID issued from a recognized government agency or business organization. All non-U.S. born citizens must possess the original proof of citizenship. All visits by foreign nationals must be approved in advance, and the visitor must possess their original passport or visa as proof of identification and legal status.

(2) Individuals who access the Laboratory on a regular basis for business related activities but do not occupy JPL office space may be provided a non-embossed picture badge. This badge allows the individual to access JPL through any security-staffed entry gate and allows parking in any outside lot including the Visitor Lot. Prior to the individual receiving this badge, the Subcontractor must submit JPL Form 2190, “Affiliate Start/Separation Notice,” to the JPL Security Office. This form is available from the JPL Security Office.

(k) The Subcontractor shall notify the JPL Subcontracts Manager no later than the end of the day of the termination for cause of an authorized Subcontractor personnel’s access. The Subcontractor shall notify the JPL Subcontract Manager and the designated JPL Contract Technical Manager no later than ten days after an authorized Subcontractor personnel no longer requires access for any other type of termination. Identification badge and any other JPL/NASA assets possessed by the terminated Subcontractor employee will be retrieved by the Subcontractor prior to the departure of the Subcontractor employee from the work site. The JPL/NASA badge and property will be turned in to the JPL Security Office within 24 hours after termination by the Subcontractor. Verbal notifications of termination action will be confirmed in writing within 30 days.

(l) The Subcontractor must ensure that any forms required for personnel investigations/National Agency Checks are completed by the individuals who are to perform work under this Subcontract as requested by JPL in order to determine eligibility for access to sensitive material or controlled facilities.

(m) Incorporated documents are available through the “Miscellaneous Subcontractor Documents” link on the JPL Acquisition Home Page at the following URL:

http://acquisition.jpl.nasa.gov/e2000.htm

(n) The Subcontractor shall ensure that its employees, in performance of the Subcontract, receive annual IT security training in NASA IT Security policies, procedures, computer ethics, and best practices in accordance with NPG 2810.1, Section 4.3 requirements. The Subcontractor may use web-based training available from NASA to meet this requirement.

(o) The Subcontractor shall incorporate the substance of this clause in all First-tier Subcontracts that meet the conditions in paragraph (a) of this clause.